IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: **5640 CEDAR AVENUE, PHILADELPHIA, PENNSYLVANIA 19143; THE PERSON OF ANTHONY DAVID ALE SMITH; and ELECTRONIC DEVICES**	MAGISTRATE NO. 20-1748-ALL **FILED UNDER SEAL**

CONSOLIDATED AFFIDAVIT IN SUPPORT OF APPLICATIONS UNDER RULE 41 FOR THREE WARRANTS TO SEARCH AND SEIZE

I, LAUREN LAIELLI, Task Force Officer, Joint Terrorism Task Force, Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this consolidated affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search 1) the residence of ANTHONY DAVID ALE SMITH, that is, the premises known as 5640 Cedar Avenue, Philadelphia, PA 19143, hereinafter "PREMISES," further described in Attachment A-1, for the things described in Attachment B-1; 2) the person of ANTHONY DAVID ALE SMITH, hereinafter "SMITH," further described in Attachment A-2, for the things described in Attachment B-2; and for all cell phones, computers, tablets, and other electronic storage media belonging to, or in the custody and control of, SMITH, as described in Attachment A-3, for the things described in Attachment B-3.

2. On October 20, 2020, SMITH, along with two other individuals discussed below, were indicted by a grand jury sitting in the Eastern District of Pennsylvania in a three-count indictment, charging SMITH and his co-defendants with one count of arson of property belonging to an agency that receives federal funding, and aiding and abetting, in violation of 18

U.S.C. §§ 844(f)(1), (2) and 2; one count of arson affecting interstate commerce, and aiding and abetting, in violation of 18 U.S.C. §§ 844(i) and 2, and one count of obstruction of law enforcement during a civil disorder, and aiding and abetting, in violation of 18 U.S.C. §§ 231(a)(3) and 2. This search warrant seeks authorization to search for evidence of these crimes, as discussed below.

3. I am a sworn law enforcement officer employed by the New Jersey Office of Homeland Security and Preparedness, hereinafter "NJOHSP". I have been a member of the NJOHSP since July 2015. I have been a sworn law enforcement officer since 2010. I am presently assigned full-time as a Task Force Officer, hereinafter "TFO" with the FBI Philadelphia Joint Terrorism Task Force, hereinafter "JTTF", South Jersey Resident Agency. As an FBI TFO and member of the JTTF, I have been duly deputized as a federal law enforcement officer, which authorizes me to investigate violations of federal criminal law. During my time as a law enforcement officer, I have conducted numerous investigations involving various criminal acts, including violent crime, of various individuals and organizations, and have authored numerous search and arrest warrants.

4. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit is intended to show merely that there is sufficient

probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the information outlined in this affidavit, as well as my training and experience, there is probable cause to believe that the PREMISES and the person of SMITH contain evidence of violations of 18 U.S.C. § 844(f)(1) and (f)(2) (knowing, intentional, and malicious damage and destruction, and attempted damage and destruction, by means of fire, a vehicle, and other real and personal property, which was owned and possessed by an institution or organization receiving Federal financial assistance, that is, a Philadelphia Police Department vehicle, and created a substantial risk of injury to any person); 18 U.S.C. § 844(i) (arson affecting interstate commerce), and 18 U.S.C. § 231(a)(3) (obstruction of law enforcement and interstate commerce during a civil disorder), § 2 (aiding and abetting).

6. The Philadelphia Police Department receives federal funding. Specifically, in May 2020, the Philadelphia Police Department was in receipt of federal funding from the Edward Byrne Memorial Justice Association Grant ("JAG"), identified as grants DJBX-0727, and DJBX-0465.

BACKGROUND OF ARSON INVESTIGATION

7. On or about May 25, 2020, George Floyd died while in the custody of the Minneapolis, Minnesota, Police Department. The circumstances surrounding Floyd's death drew national media attention. In the days following Floyd's death, large-scale protests were held throughout the United States.

8. One such protest took place on or about Saturday, May 30, 2020, in and around Philadelphia, Pennsylvania. While the protest earlier in the day was peaceful, violence erupted later in the day. Among other things, a group of individuals began to riot, smashing store fronts, looting stores, and attacking multiple marked Philadelphia Police Department, hereinafter "PPD" vehicles. These vehicles included one PPD sedan (number C-109) near the Municipal Services Building, which was set on fire at approximately 5:40 p.m. This vehicle was destroyed as a result of being set on fire. This is how the vehicle appears after the fire:

9. During the course of the investigation, I, together with other investigators, have gathered thousands of video and photographic pieces of evidence for review in an attempt to identify the individuals responsible for the arson of C-109. The evidence reviewed included the time frame of the arson, as well as before and after the arson in an attempt to track the subjects of the investigation.

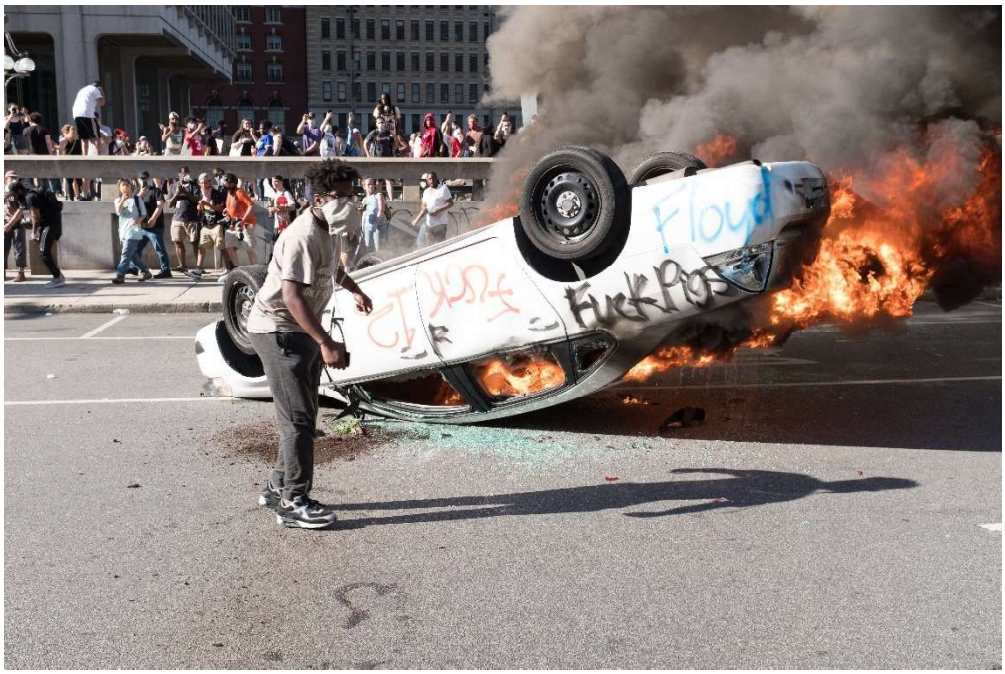
10. Through review of publicly available news outlet and social media photographs, videos, and footage, and general internet research, three individuals were identified as directly involved in the arson of the PPD vehicle described above. These individuals were identified as SMITH; CARLOS MATCHETT, hereinafter "MATCHETT"; and KHALIF MILLER, hereinafter "MILLER". On October 20, 2020, these three individuals were indicted by a grand jury sitting in the Eastern District of Pennsylvania in a three-count indictment, charging all three defendants with one count of arson of property belonging to an agency that receives federal funding, and aiding and abetting, in violation of 18 U.S.C. §§ 844(f)(2) and 2; one count of arson affecting interstate commerce, and aiding and abetting, in violation of 18 U.S.C. §§ 844(i) and 2, and one count of obstruction of law enforcement during a civil disorder, and aiding and abetting, in violation of 18 U.S.C. §§ 231(a)(3) and 2.

11. In footage available to the government, MILLER is seen adding combustible materials to car C-109. He additionally is seen with a water bottle filled with a reddish-brown liquid, which may be accelerant. MATCHETT is seen putting lighter fluid on C-109, and adding combustible materials to C-109. SMITH is observed adding what appears to be paper or cardboard and moving other kindling objects in the vehicle. Additionally, review of photographs available show that a lighted road flare was placed inside the vehicle. The investigation continues as to which individual placed the flare inside the vehicle.[1]

---

[1] Review of photographs and video taken that day is ongoing, and additional individuals aiding and abetting in the arson of this police car may be identified in the future.

12. I have examined additional video and photographs obtained by law enforcement. These videos and photographs include, but are not limited to, the following photograph, which shows SMITH in front of C109, upside-down and on fire:



13. In this picture, and others from the time of the arson, SMITH can be seen wearing a light colored shirt with lettering on the front that appears to reads "WHEN I WAS 11, I TURNED 13 CUZ ION F*CK WITH 12.", gray sweatpants, a light-colored, striped facemask with ties on the top and the bottom, black and white sneakers, which appear to be NIKE brand, and large framed, dark-colored glasses.

14. On September 15, 2020, a Search Warrant was signed by the Honorable Carol Sandra Moore Wells for SMITH's Instagram account. The results from this search warrant

included various memes and postings encouraging violence against the police. The following image from the day of the arson, showing SMITH sitting on top of the upside-down C109 was also found pursuant to the search warrant:

THE PREMISES AND SUBJECT ELECTRONIC DEVICES

15. Based upon investigation and information available to me, SMITH lives at the PREMISES, 5640 Cedar Avenue, Philadelphia, PA 19143. He has been observed at this

residence by law enforcement in the past several weeks, both exiting the PREMISES and returning to it. He was seen as recently as October 23 and 25, exiting the house and reentering it, and using a key to do so. A Postal Inspector with the United States Postal Inspection Service has verified that SMITH has registered for a postal account at the PREMISES, and that he has registered for text alert updates with the Postal Service using the phone number 267-266-8031, which, as discussed below, matches information from the cell phone provider and social media accounts as to SMITH's usage of the phone. The home is owned by Romeo Anthony Smith, a man who is 54 years old. Additionally, in an Instagram message dated June 3, 2020, SMITH tells an unknown individual with a username of "canyounotalicia" that his address is "5640 cedar Avenue". In addition to SMITH, about three minor children, one unknown black female, one black female believed to be Alicia Pinnock,[2] and two unknown black adult males were also observed at the residence.[3]

16. Based on my training and experience, I know that individuals who commit crimes, including arson, often maintain items related to their crimes including those specified in Attachments B-1 and B-2, which are incorporated herein, within their homes and/or their person. These items often include clothing items or personal effects used during the commission of the

---

[2] This female matches the physical appearance of the woman whose picture is associated with the "canyounotalicia" Instagram user. Additionally, a car registered to Alicia Pinnock has been observed outside the house.

[3] SMITH does have a photo identification card through the Pennsylvania Department of Motor Vehicles. This identification was last renewed in September 2018, and reflects an older address tied to SMITH, in Sharon Hill, PA.

crimes. Here there is probable cause to believe that SMITH will maintain in his home or on his person items seen in the videos and photographs described above, and detailed in Attachments B-1 and B-2, including the light colored shirt with lettering on the front, the gray sweatpants, the light colored, striped facemask with ties on the top and the bottom, the black and white sneakers, which appear to be NIKE brand, and the large framed, dark-colored glasses.

17. Additionally, individuals who commit crimes often use cellular telephones, to include primary, secondary, and/or burner phones, for communication with co-conspirators and aiders and abettors for research on target locations and for planning escape routes, among other facets to their criminal activity. Cellular phones that can be purchased for cash or without providing much identifying information, commonly known as "burner phones," are used by criminals during the commission of crimes due to their perceived anonymity. I also know that companies that furnish burner phones do not require an individual to provide any identifying information for the user. Based on my training and experience, in general the carrying of cell phones is almost ubiquitous.[4] In addition, SMITH was observed on the day of the arson holding a cellular phone while sitting on top of C109 (the photo shown above).

---

[4] *See Carpenter v. United States*, 138 S.Ct. 2206, 2211 (2018) (stating that, as of approximately June 2018, "there were 396 million cell phone service accounts in the United States—for a Nation of 326 million people"); *Riley v. California*, 572 U.S. 373, 395 (2014) (stating statistics show 90% of American adults own a cellular phone, and nearly three-quarters of smart phone users reported being within five feet of their phones most of the time). In *Carpenter*, the Court found that Americans have a "compulsive[]" need to carry and use their cellular phones:

18. As a result of SMITH having a phone present on May 30, it is probable that he used this phone to either communicate with others about his crimes, or to take pictures or other documentation of his activities on May 30. Subscriber information and social media returns have shown that SMITH has used at least one cell phone, operated by T-Mobile, and with phone number 267-266-8031.

19. Additionally, smart phones, computers, tablets, and other electronic devices can access the internet. In this case, there is probable cause to believe that searching of SMITH's cell phone(s), tablets, computers, and other electronic devices will provide evidence of communication between co-conspirators and aiders and abettors. Information regarding the purchase of other items seem in the video, including the light-colored shirt with lettering on the front, the gray sweatpants, the light-colored, striped facemask with ties on the top and the bottom, the black and white sneakers, which appear to be NIKE brand, and the large framed, dark-colored glasses. Additionally, SMITH may use these devices to access his social media

---

> A cell phone—almost a "feature of human anatomy"—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.

Carpenter, 138 S.Ct. at 2218 (citations omitted).

accounts, as discussed above. As discussed above, SMITH posted pictures of himself near the car that was set on fire to his social media.

20. Individuals often communicate with co-conspirators and aiders and abettors before, during, and after they commit crimes. In this case, there is probable cause to believe that the searching of SMITH's cell phone(s), tablets, computers, and other electronic devices will provide evidence of communication between SMITH and any co-conspirators and aiders and abettors regarding the arsons that were committed.

21. Individuals often communicate their planning, execution, and motivation for committing crimes such as arsons to co-conspirators and aiders and abettors. This can occur through text, use of phone "apps," social media websites, and other internet resources accessible via smart phone, tablet, or computer. It can also occur in handwritten documents, or other physical media.

22. Here, there is probable cause to believe that evidence as to SMITH's planning and motivation for committing the arsons on May 30, 2020 will be found in a search of his cell phone, as well as any other electronic devices found in his possession or at his home. His motivation for doing so is currently unknown.

23. Additionally, there is probable cause to believe that SMITH utilized these devices to communicate with any co-conspirators and aiders and abettors, and to inform individuals in his success with the arson after it occurred.

TECHNICAL TERMS

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

29. As described above and in Attachments B-1, B-2, and B-3, these applications seek permission to search for information that might be found on the PREMISES, on the person of SMITH, and on his electronic devices, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

30. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, or on the person of SMITH, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on actual inspection of other evidence related to this investigation, including the video footage uploaded to YouTube, I am aware that computer equipment was used to generate, store, and upload video files, photographs, and/or documents that are evidence of the violations specified above. There is reason to believe that there is a computer and/or computer system currently located on the PREMISES.

31. *Forensic evidence.* As further described in Attachment B-3, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information

about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic

storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement). A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on

other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

d. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained

above, because the warrants calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

33. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-

assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

34. Because several people may share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in the warrants could be found on any of those computers or storage media, the warrants applied for would permit the seizure and review of those items as well.

CONCLUSION

35. I submit that this affidavit supports probable cause for warrants to search the PREMISES described in Attachment A-1 and seize the items described in Attachment B-1, to search the person of SMITH described in Attachment A-2 and seize the items described in Attachment B-2, and to seize the items described in Attachment A-3 and seize the items described in Attachment B-3 for evidence of violations of 18 U.S.C. § 844(f)(1) and (f)(2) (knowing, intentional, and malicious damage and destruction, and attempted damage and destruction, by means of fire, a vehicle, and other real and personal property, which was owned and possessed by an institution or organization receiving Federal financial assistance, that is, a Philadelphia Police Department vehicle, and created a substantial risk of injury to any person); 18 U.S.C. § 844(i) (arson affecting interstate commerce) and 18 U.S.C. §§ 231(a)(3) (obstruction of law enforcement and interstate commerce during a civil disorder), § 2 (aiding and abetting).

REQUEST FOR SEALING

38. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of these applications, including the applications and search warrants. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

/Lauren Laielli
LAUREN LAIELLI
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me
on October 26, 2020:

/s Richard A. Lloret
HONORABLE RICHARD A. LLORET
United States Magistrate Judge

ATTACHMENT A-1

PROPERTY TO BE SEARCHED

5640 Cedar Avenue, Philadelphia, PA 19143

DESCRIPTION: 5640 Cedar Avenue, Philadelphia, PA 19143. The property is a two-story row home attached on one side. The residence is constructed of brick and yellow siding. The house has a front porch (not enclosed, but covered).

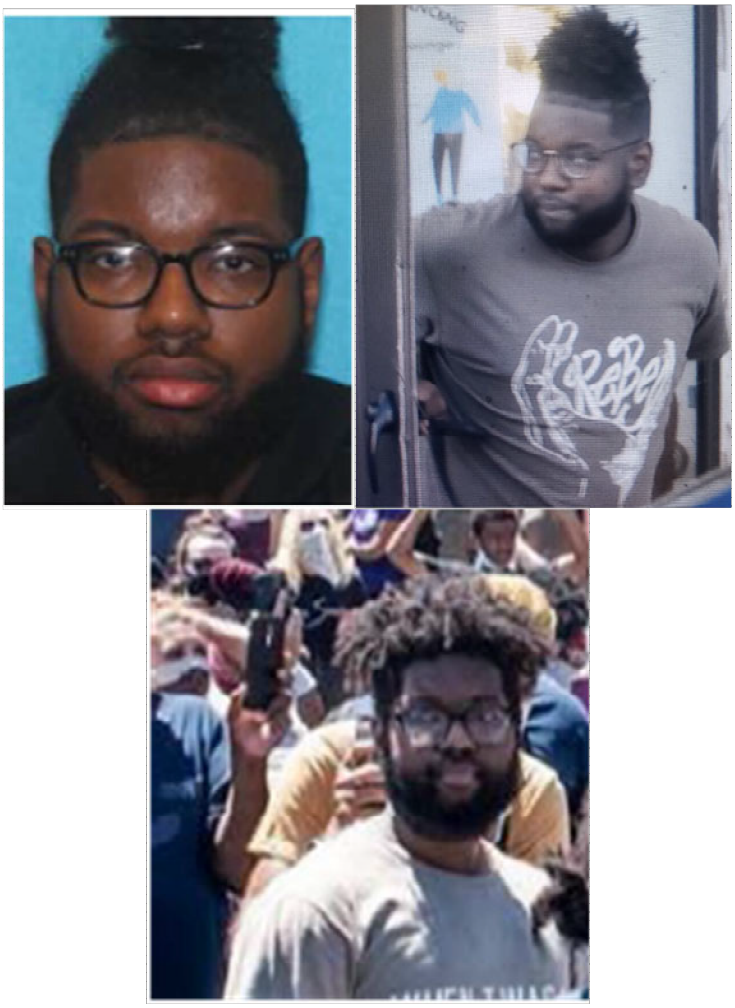
ATTACHMENT A-2

PERSON TO BE SEARCHED

ANTHONY DAVID ALE SMITH

DESCRIPTION: ANTHONY DAVID ALE SMITH, black male, approximately 5'7" in height, heavy build, DOB: [redacted]

Below from left to right are: a DMV photo of SMITH (date unknown), a photo from the past few weeks, and a photo from May 30, 2020:



ATTACHMENT A-3

PROPERTY TO BE SEARCHED

TELEPHONES, COMPUTERS, TABLETS, AND OTHER ELECTRONIC DEVICES

Any cellular telephones, computers, tablets, and other electronic devices capable of accessing the internet, belonging to, or in the custody or control of SMITH's person at the time of the aforementioned search of 5640 Cedar Avenue, Philadelphia, PA, or SMITH's person.

ATTACHMENTS B-1 and B-2

ITEMS TO BE SEIZED

1. The following items which are evidence of or property used to commit violations of 18 U.S.C. § 844(f)(1) and (f)(2) (knowing, intentional, and malicious damage and destruction, and attempted damage and destruction, by means of fire, a vehicle, and other real and personal property, which was owned and possessed by an institution or organization receiving Federal financial assistance, that is, a Philadelphia Police Department vehicle, and created a substantial risk of injury to any person); 18 U.S.C. § 844(i) (arson affecting interstate commerce) and 18 U.S.C. §§ 231(a)(3) (obstruction of law enforcement and interstate commerce during a civil disorder), § 2 (aiding and abetting), as described in the Affidavit in Support of Search Warrant:

A. Light-colored shirt with lettering on the front;

B. Gray sweatpants with pockets;

C. Light-colored, striped facemask with ties on the top and the bottom;

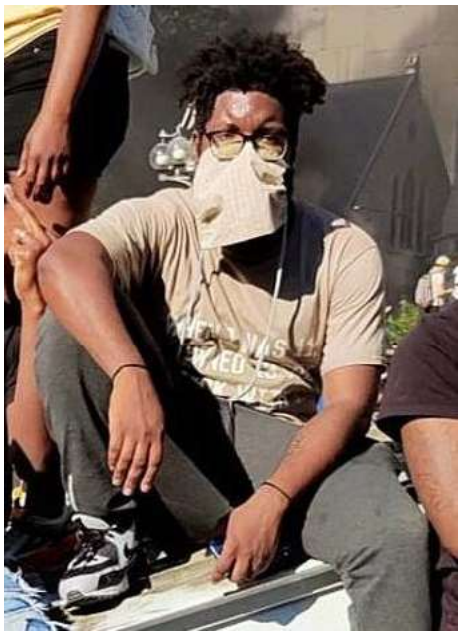
D. Black and white sneakers (appearing to be Nike brand);

E. Large framed, dark-colored glasses;

F. Indicia of residency, to include bills or documents of SMITH;

G. Cellular telephones, computers, tablets, and other electronic devices

Images of items A through E are below:



ATTACHMENT B-3

ITEMS TO BE SEIZED

1. All records relating to violations of 18 U.S.C. § 844(f)(1) and (f)(2) (knowing, intentional, and malicious damage and destruction, and attempted damage and destruction, by means of fire, a vehicle, and other real and personal property, which was owned and possessed by an institution or organization receiving Federal financial assistance, that is, a Philadelphia Police Department vehicle, and created a substantial risk of injury to any person); 18 U.S.C. § 844(i) (arson affecting interstate commerce), 18 U.S.C. §§ 231(a)(3) (obstruction of law enforcement and interstate commerce during a civil disorder), and § 2 (aiding and abetting), as described in the Affidavit in Support of Search Warrants, including:

a. Indicia of ownership or possession;

b. Records, electronic files, video footage, photographs, communications, correspondence, and information depicting and/or related to the destruction of a PPD vehicle on or about May 30, 2020, in the vicinity of City Hall, in Philadelphia, PA;

c. Evidence of planning, motivation, and research on commission of arson; and

d. Evidence of the purchase of the following items: the light-colored shirt with lettering on the front, the gray sweatpants, the light-colored, striped facemask with ties on the top and the bottom, the black and white sneakers, which appear to be NIKE brand, and the large framed, dark-colored glasses;

e. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER");

f. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

g. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

h. Evidence of the lack of such malicious software;

i. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

j. Evidence indicating the computer user's state of mind as it relates to the crime under investigation;

k. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

l. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

m. Evidence of the times the COMPUTER was used;

n. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

o. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

p. Records of or information about Internet Protocol addresses used by the COMPUTER;

q. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

r. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.